AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions and listings of claims in the application:

Claims 1-8 canceled.

9. (Currently Amended) **A modular arithmetic apparatus for performing an arithmetic operation of an integer on a basis of a residue number system (RNS), comprising:**

an input/output unit configured to input data included in modulus p and to output an arithmetic result;

a storage unit configured to store at least a portion of a plurality of base parameter sets, each base parameter set including a set of base parameters indicating base elements, each one of said plurality of base parameter sets containing a different number of base parameters;

a base selection unit configured to select one base parameter set in said storage unit according to the modulus p input from said input/output unit; and

a plurality of arithmetic units configured to perform operations in parallel according to the selected one base parameter set to obtain the arithmetic result,

~~**The apparatus of claim 5,**~~ wherein the numbers of the base parameters of each base parameter set in said storage unit are multiples of {u-t, u-t+1, - - - , u}, respectively, said u is a number of the arithmetic units and said t is a maximum integer of a number of unused ones of the arithmetic units (t=0 or 0<t<u).

Claims 10-19 canceled.

20. (Currently Amended) **A modular arithmetic method of performing an arithmetic operation of an integer on a basis of a residue number system (RNS) by a plurality of operation units in parallel, the method comprising:**

storing at least a portion of a plurality of base parameter sets to a storage unit, each base parameter set including a set of base parameters indicating base elements, each one of said plurality of base parameter sets containing a different number of base parameters inputting data included in modulus p;

selecting one base parameter set in said storage unit according to the input modulus p;

performing operations in parallel by the plurality of operation units according to a set of base parameters indicating the selected one base parameter set to obtain an arithmetic result; and

outputting the obtained arithmetic result,

~~**The method of claim 16,**~~ wherein the numbers of the base parameters of each base parameter set in said storage unit are multiples of {u-t, u-t+1, . . . , u}, respectively, said u is a number of the arithmetic units and said t is a maximum integer of a number of unused ones of the arithmetic units (t=0 or 0<t<u).